

GSA POLICY AND PROCEDURE

SUBJECT: Meetings with Representatives of Foreign Governments or Foreign Industry,
Foreign Travel, and Foreign Contacts

1. Purpose. This General Services Administration (GSA) policy establishes procedures and employee reporting requirements for the following: (1) meetings/visits with representatives from foreign governments and/or foreign industry; (2) foreign travel; and (3) foreign contacts.

2. Applicability. This policy applies to all GSA employees, including, but not limited to, full-time and part-time employees, interns, and employees of other agencies on detail to GSA. It does not apply to the OIG to the extent the OIG determines that it is inconsistent with OIG policies, independence, and mission.

3. Background.

- We operate in an environment where foreign governments and others continue to invest considerable time and resources to assessing and targeting U.S. Government employees for both recruitment and the transfer of vital Government information. Transfer attempts are devised both knowingly and unknowingly through a targeted individual, often seeking information that is unclassified yet sensitive in nature when compiled from multiple sources or over a sustained time period.
- Presidential Decision Directive PDD/NSC-12 states that a mainstay of foreign intelligence services is the recruitment of well-placed assets, such as U.S. Government employees, who can provide insightful intelligence on a particular issue. The United States is, and will continue to be, the prime focus of Foreign Intelligence Services. Therefore, those in the Federal workforce, especially those in sensitive positions, are of special interest to Foreign Intelligence Services.
- This policy is not intended to limit or impair professional or personal contacts. Rather, its purpose is to protect the security of the United States and its employees while ensuring privacy of employees and their freedom of association. This policy ensures that security risks to individuals or to the U.S. Government are identified at the earliest opportunity and deterred.
- This policy is designed to protect GSA and its employees against foreign government exploitation, while also preventing unauthorized access to classified, sensitive, and proprietary information.

4. Meetings/visits with representatives of foreign governments or foreign industry.

- Representatives of a foreign government or foreign industry who participate in meetings/visits at GSA facilities or with GSA employees could pose a security risk. It is an opportunity for visitors to solicit and collect information that is not readily available and an opportunity for them to identify points of contact and recruit personnel to provide information in the future.
- Any GSA employee who receives a request for a meeting/tour from a foreign government or foreign industry must notify the Office of Congressional and Intergovernmental Affairs (OCIA). OCIA will coordinate with the Department of State and other Federal agencies as applicable, and for approved visits, will become the lead point of contact with the foreign government officials.
- Any GSA office/employee who hosts a meeting/tour that includes one or more representatives from a foreign government or foreign industry must submit a meeting request in coordination with OCIA to the Threat Management Office (TMO) or Chief Security Officer (CSO) in the Office of Mission Assurance. The meeting request must be submitted at least 7 business days prior to the visit, and the information listed in the attached appendix must be included. In the case of repeat or recurring visits by the same representative(s) of a foreign government or foreign industry, a request must be resubmitted for each meeting/visit.
- The CSO will review the meeting/visit request and make a recommendation to OCIA and the hosting GSA office/employee for or against the meeting/visit.
- Prior to the visit, the CSO will coordinate the planning of the meeting with the hosting office/employee and OCIA. OCIA or the hosting office/employee will contact the foreign visitor(s) and request that they bring proper identification to the meeting. They will also advise the representative(s) of foreign governments or foreign industry that no electronic devices—including cameras and cellular telephones—can be brought to the meeting/visit.
- On the day of the meeting/visit, the identity of the representative(s) of foreign governments or foreign industry will be verified by a GSA hosting office/employee before access is permitted to the GSA facility. When applicable, all electronic devices that are brought by the representative(s) of foreign governments or foreign industry will be collected and securely stored until the meeting/visit is concluded. (This occurs from time to time when an individual inadvertently brings an electronic device although advised not to do so.)
- It is the responsibility of the GSA hosting office/employee to ensure that the representative(s) of foreign governments or foreign industry are escorted and closely monitored at all times while they are visiting GSA facilities. The hosting office/employee must also ensure that representative(s) of foreign governments or foreign industry are not allowed access to any GSA information technology system(s) for any reason. Additionally, all electronic devices (such as flash drives, CDs, cameras, or other media devices) from a representative of a foreign governments or foreign industry must never be used in Government computers or other devices. (Note: Per policy above, electronic devices are not to be brought to the meeting/visit.)

- The CSO must be notified that the meeting/visit has concluded and that all visitor badges have been collected. Any gift from a representative of a foreign government or foreign industry that is an electronic device must be submitted to the CSO for inspection and inventory. A debriefing of the hosting employee and other GSA employees who were meeting/visit participants may be conducted by the CSO if necessary.

5. Foreign Travel.

- GSA employees with a security clearance (e.g., secret, top secret) are required to provide notice to the TMO of all foreign travel, conducted for either official or personal purposes, at least 2 weeks in advance of travel. Foreign travel is defined as travel outside the United States and its Territories. Such employees may be required to receive a travel briefing prior to foreign travel and may be subject to a security debrief upon completion of foreign travel.
- GSA employees without a security clearance are encouraged but not required to notify the TMO of all foreign travel, conducted for either official or personal purposes. Such employees may receive travel briefings prior to foreign travel and may be asked to participate in a security debrief upon completion of foreign travel.
- GSA employees are prohibited from taking Government-furnished electronic devices (laptops, tablets, phones) on foreign travel unless cleared by the CSO and IT support (OCIO).

6. Foreign Contacts.

- GSA employees are required to report all contacts with foreign citizens, of any nationality, to the TMO if either or both of the criteria below are met. This requirement applies to contacts that take place while inside or outside the United States and its Territories, and both within or outside the scope of an employee's official duties:
 - Illegal or unauthorized access is sought to classified or otherwise sensitive information which the requesting individual is not authorized to receive; and/or
 - The employee is concerned that he/she may be a target of actual or attempted exploitation by a foreign entity.
- Report content for reportable foreign contacts includes the following information:
 - The name of the employee who had the contact, the date and location of the contact, and the general circumstances of the contact. If the contact involved a request to receive information that the individual is not authorized to receive, the specific content of the conversation and a description of the requested information and/or documents must be reported; and
 - If known, the name and description of the suspicious individual(s).

7. Additional Information. Questions regarding this Directive should be addressed to the Chief Security Officer at (threat-management-office@gsa.gov) or the Office of Mission Assurance at eoc@gsa.gov.

8. Signature.

DAN TANGHERLINI
Administrator

June 12, 2014
Date

Appendix

APPENDIX

Requests for hosting meetings and visits with representatives of foreign governments or foreign industry must contain the following information:

Foreign Visitor Identifying Data.

- Visitor's Full Name (First, Middle, Last).
- Gender.
- Country of Origin/Citizenship.
- Date of Birth (MM/DD/YYYY).
- Place of Birth (City and Country).
- Passport or Visa Number:
 - Country That Issued Passport.
 - Issuance Date.
 - Expiration Date.
- Visitor Organization/Employer.
- Purpose of Meeting:
 - Meeting Start Date and Time.
 - Meeting End Date and Time.
 - Building(s) and Room Number(s) to be Visited.
- Hosting Official (Name, Title, Building, Room Number, and Phone Number).
- Escort Information (If different from hosting official).
- Proposed Discussion Topics.